# ○学校法人東京電機大学情報セキュリティ対策規程

情報統括責任者<br>総合メディアセンター

## 第１章　総則

（目的）

第１条　本規程は、学校法人東京電機大学情報セキュリティ基本規程（以下「基本規程」という。）に基づき、本法人において実施すべき情報セキュリティ対策の具体的内容、方法及び運用上の基準を定め、情報資産の機密性、完全性及び可用性を確保することを目的とする。

（適用範囲）

第２条　本規程は、基本規程第３条に規定する利用者及び委託先に適用する。

（実施体制）

第３条　本規程に基づく情報セキュリティ対策は、基本規程第５条に規定する情報セキュリティ最高責任者（CISO）の統制の下、基本規程第７条に規定する情報セキュリティ統括本部が、全学的観点から必要な調整及び指示を行う。

２　基本規程第９条に規定する情報セキュリティ統括実施機関（以下「統括実施機関」という。）の長である情報セキュリティ実施責任者は、前項に規定する統制及び調整に基づき、本規程に定める情報セキュリティ対策の具体的な企画、実施、運用及び改善を統括する。

３　情報システム管理責任者は、所管する情報システム及び情報資産について、統括実施機関と連携し、本規程に基づく対策を具体的に実施する。

４　利用者は、本規程及び関係規程並びに関係者の指示に従い、情報資産を適切に取り扱わなければならない。

## 第２章　情報資産の分類及び管理

（情報資産の分類）

第４条　基本規程第11条の規定に基づき、情報資産は、その内容及び重要度に応じ、次の各号に掲げる区分に分類する。

（１）非公開情報資産

（２）限定公開情報資産

（３）公開情報資産

２　前項の分類基準及び具体的取扱方法は、別に定める。

（情報資産の取扱い）

第５条　情報システム管理責任者は、非公開情報資産について、不特定者のアクセス、盗難、漏えい、改ざん又は滅失を防止するため、暗号化、アクセス制御その他必要な情報セキュリティ対策を講じなければならない。

２　情報システム管理責任者は、限定公開情報資産について、認証及びアクセス制御により管理し、必要に応じて利用状況を確認しなければならない。

３　情報システム管理責任者は、公開情報資産について、改ざん又は破壊を防止する措置を講ずるとともに、個人情報、プライバシー及び著作権その他の法令上保護される権利に配慮しなければならない。

（情報資産の管理）

第６条　情報資産は、原則として、当該情報資産を保有し、又は保管する部署等の情報システム管理責任者が管理するものとする。

２　情報システム管理責任者は、所管する情報資産を第４条で定めた区分に分類し、前条に定める情報資産の取扱い状況を把握し、次に掲げる事項を明確にした上で、必要な情報セキュリティ対策を実施しなければならない。

（１）管理責任者

（２）保管場所及び保存方法

（３）利用可能な者及び利用方法

（４）外部提供及び学外持ち出しの可否

（５）保存期間及び廃棄方法

３　情報システム管理責任者は、統括実施機関から求めがあったとき、又は必要があると認めるときは、対策の実施状況を報告しなければならない。

４　利用者は、情報資産の分類及び取扱い区分を認識し、当該分類に応じて適切に利用しなければならない。

（保管及び学外持ち出し）

第７条　非公開情報資産及び限定公開情報資産は、その重要度に応じ、認証及びアクセス制御その他の適切な情報セキュリティ対策が施された環境に保管しなければならない。

２　情報資産を学外へ持ち出す場合は、教育、研究又は業務上の必要性を確認した上で、暗号化その他の情報漏えい防止措置を講じなければならない。

３　外部クラウドサービスその他外部環境に情報資産を保存する場合についても、前２項の規定を準用するものとする。

（情報機器及び記録媒体の管理及び廃棄）

第８条　情報機器及び記録媒体は、その利用目的及び取り扱う情報資産の重要度に応じ、適切に管理しなければならない。

2　情報機器及び記録媒体を廃棄し、又は譲渡する場合は、当該情報が第三者により復元されることのないよう、消去、物理的破壊その他適切な措置を講じなければならない。

## 第３章　アクセス権及びアクセス管理

（アカウント管理）

第９条　情報資産の利用に当たっては、情報資産毎に利用者固有のアカウントを付与するものとする。

2　アカウントの共用は原則禁止する。やむを得ない場合に限り、必要最小限とし、その管理責任者を明確にしなければならない。

3　アカウントの管理（発行、変更、停止、削除等）は、情報システム管理責任者の責任において適切かつ速やかに行わなければならない。

（アクセス権の付与）

第10条　アクセス権の付与は、情報システム管理責任者の承認の下、利用目的及び職務内容を確認した上で行わなければならない。

2　アクセス権は、利用目的の達成に必要な最小限の範囲に限定しなければならない。

（アクセス権の変更及び削除）

第11条　情報システム管理責任者は、利用者の職務内容、役割、所属、身分又は資格に変更があった場合には、速やかにアクセス権を変更し、又は削除しなければならない。

（認証情報の管理）

第12条　利用者は、自己の認証情報を厳重に管理し、第三者に開示し、又は漏えいしてはならない。

2　認証情報の具体的な管理方法については、統括実施機関が別に定めることができる。

## 第４章　システム及び端末の運用管理

（サーバ及びネットワーク管理）

第13条　基幹ネットワーク及び主要なサーバは、基本規程第９条に規定する統括実施機関が管理する。

2　学部、学科、学系、系、研究室、中学校・高等学校及び各部署等で設置される情報システムについては、当該情報システム管理責任者が管理する。

3　情報システムの管理に当たっては、ファイアウォールやその他のセキュリティ対策ツールを適切に運用し、不正アクセス等に対処しなければならない。

（ログ管理）

第14条　情報システム管理責任者及び統括実施機関は、それぞれ所管する情報システムについて、適切な運用及び情報セキュリティインシデントの検知・分析を目的として、次に掲げるログを取得しなければならない。

（１）サーバ及びネットワーク機器における通信及び操作に関するログ

（２）認証及びアクセス制御に関するログ

（３）その他、情報セキュリティ確保のために必要と認められるログ

２　前項のログは、改ざん又は消去されることのないよう適切に管理し、一定期間保存しなければならない。

３　情報システム管理責任者及び統括実施機関は、情報セキュリティ最高責任者又はセキュリティインシデント対応チーム（以下「TDU-CSIRT」という。）から、情報セキュリティの確保又はインシデント対応に必要な範囲でログの提供を求められた場合には、正当な理由がない限り、速やかにこれを提供しなければならない。

（バックアップ）

第15条　情報システム管理責任者は、障害、誤操作、災害等に備え、重要な情報資産について、必要に応じて定期的にバックアップを行うものとする。

２　バックアップの対象、方法及び取得頻度は、情報システム管理責任者が、情報資産の重要度及び利用形態に応じて定めるものとする。

３　情報システム管理責任者は、必要に応じて、バックアップデータからの復元が可能であることを確認しなければならない。

（端末管理）

第16条　学内ネットワークに接続する端末は、統括実施機関が定める情報セキュリティ対策が講じられたものでなければならない。

２　前項の規定に基づく情報セキュリティ対策については、法人資産端末及び私物端末の区分に応じて、その管理方法及び対策内容を定めるものとする。

（私物端末の取扱い）

第17条　学内ネットワークに接続する私物端末については、次に掲げる最低限の情報セキュリティ対策を講じなければならない。

（１）基本ソフトウェア及び主要なアプリケーションを最新の状態に保つこと

（２）不正プログラム対策その他の基本的なセキュリティ対策を講じること

（３）第三者による不正利用を防止するための措置を講じること

２　前項の対策が講じられていないと認められる場合には、統括実施機関は、当該端末の学内ネットワークへの接続を制限することができる。

（法人資産端末における必須対策）

第18条　法人資産端末については、統括実施機関が定める端末管理及び不正アクセス防止

その他必要なセキュリティ対策を講じなければならない。
2　前項の措置が講じられていない端末については、統括実施機関は、原則として学内ネットワークへの接続を認めない。

（ソフトウェア資産及びライセンス管理）
第19条　法人資産端末に有償のソフトウェアを導入する場合は、当該端末を所管する情報システム管理責任者は、利用状況及びライセンス情報を適切に管理しなければならない。
2　情報システム管理責任者は、所定の方法によりソフトウェアライセンス管理台帳を作成し、統括実施機関に提出しなければならない。

（サーバ等の管理状況の把握）
第20条　学内又は外部クラウドサービス等を利用してサーバその他これに準ずる情報システム（以下「サーバ等」という。）を運用する場合は、情報システム管理責任者及び当該サーバ等の管理者を明確にしなければならない。
2　前項のサーバ等については、年度ごとに所定の方法により統括実施機関に調査票を提出しなければならない。
3　前項の調査票が提出されていない場合又は内容に不備がある場合には、統括実施機関は、当該サーバ等の運用の停止、ネットワーク接続の制限その他必要な措置を講ずることができる。

（外部公開及び通信制御の申請）
第21条　学内で運用するサーバ等を学外からアクセス可能な状態で公開する場合には、情報システム管理責任者は、事前に申請を行い、統括実施機関の承認を得なければならない。
2　前項の申請があったサーバ等については、統括実施機関は、脆弱性管理の観点から必要な確認を行うものとする。
3　前項の確認により対応が必要な脆弱性が認められた場合には、統括実施機関は、情報システム管理責任者に対し、必要な是正措置を求めるものとする。
4　情報システム管理責任者において是正が行われない場合には、統括実施機関は、通信の制限又は接続の停止その他必要な措置を講ずることができる。

## 第５章　外部サービス及び委託管理

（外部サービスの利用）
第22条　外部クラウドサービスその他本法人外の情報処理サービスを利用して情報資産を処理し、又は保存する場合には、情報システム管理責任者は、当該情報資産の重要度に応じ、必要な情報セキュリティ対策が講じられていることを事前に確認しなければなら

ない。

（委託先管理）
第23条　情報システムの開発、運用管理又は情報資産の処理等を外部に委託する場合には、契約において情報セキュリティの確保及び事故発生時の報告に関する必要な事項を定めるものとする。

## 第６章　インシデント対応

（事故発生時の報告）
第24条　利用者は、基本規程第13条に基づき、情報セキュリティインシデントの発生又はそのおそれがある事象をTDU-CSIRTに速やかに報告しなければならない。

（インシデント対応）
第25条　TDU-CSIRTは、前条の報告を受けた場合、及び、情報セキュリティインシデントの発生又は発生するおそれを検知した場合には、原因の調査、影響範囲の特定と最小化、復旧及び再発防止に必要な措置を講じるものとする。
２　統括実施機関及び情報システム管理責任者は、TDU-CSIRTの指示に従い、必要な措置を講じなければならない。

## 第７章　教育及び点検

（情報倫理及び情報セキュリティ教育）
第26条　統括実施機関は、基本規程第14条に基づき、情報倫理及び情報セキュリティに関する教育を計画的に実施する。
２　前項の教育の実施方法及び内容その他必要な事項は、統括実施機関が定めることができる。

（点検）
第27条　統括実施機関は、基本規程第15条に基づき、情報セキュリティ対策の実施状況について定期的に点検を行い、その結果に応じて必要な改善措置を講じる。

## 第８章　措置

（違反時の措置）
第28条　本規程又は本規程に基づく情報セキュリティ対策に違反し、又は情報セキュリティの確保に重大な支障を及ぼすおそれがあると認められるときは、統括実施機関は、必要な範囲において、当該利用者に対し、次に掲げる措置を講ずることができる。
（１）情報システムの利用停止

（２）アクセス権の制限又は変更
（３）情報機器又は記録媒体の利用停止
（４）その他情報セキュリティの確保のため必要と認める措置
２　統括実施機関は、前項の措置を講ずるに当たり、必要に応じ当該利用者に対し、事情の説明又は資料の提出を求めることができる。
３　統括実施機関は、第１項の措置について、その必要がなくなったと認めるときは、速やかに当該措置を解除するものとする。
４　統括実施機関は、第１項の措置を講じた場合には、必要に応じ、情報セキュリティ最高責任者及び関係委員会等に報告するものとする。
５　当該事案が重大である場合は、利用者の所属部署の長その他関係部署にその旨を報告し、必要に応じ、本法人の定める規程に基づき適切な措置を講ずるものとする。

## 第９章　改廃

（改廃）
第29条　本規程の改廃は、情報セキュリティ戦略会議の議を経て行う。